

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-311826

(P2002-311826A)

(43) 公開日 平成14年10月25日 (2002. 10. 25)

(51) Int.Cl. ⁷	識別記号	F I	ターマコード [*] (参考)
G 0 9 C 1/00	6 1 0	G 0 9 C 1/00	6 1 0 A 5 B 0 3 5
	6 6 0		6 6 0 A 5 J 0 6 4
G 0 6 K 19/00		H 0 3 M 7/30	Z 5 J 1 0 4
19/07		G 0 6 K 19/00	Q
H 0 3 M 7/30			N

審査請求 未請求 請求項の数15 O L (全 11 頁)

(21) 出願番号 特願2001-116254(P2001-116254)

(22) 出願日 平成13年4月16日 (2001. 4. 16)

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(71) 出願人 000233169

株式会社日立超エル・エス・アイ・システムズ

東京都小平市上水本町5丁目22番1号

(74) 代理人 100081938

弁理士 徳若 光政

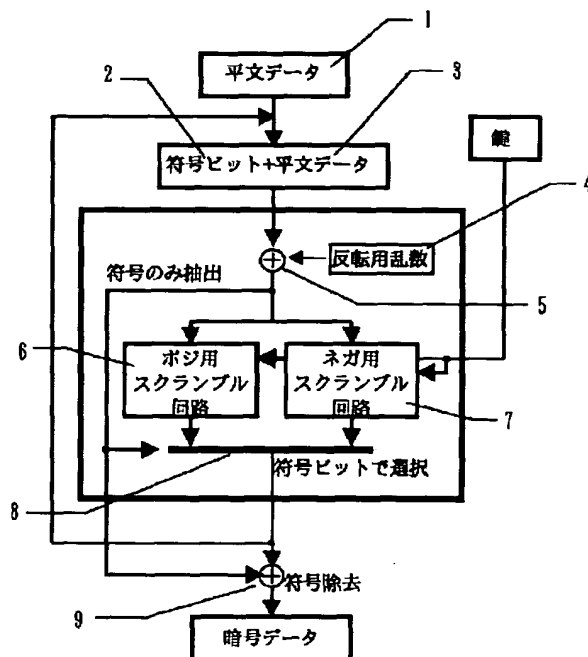
最終頁に続く

(54) 【発明の名称】 暗号化・復号化装置、暗号化・復号化方法、データの暗号化方法及びICカード

(57) 【要約】

【課題】 簡単な構成で安定的に機密保護の強化を実現した暗号化・復号化装置、暗号化・復号化方法及びICカードを提供する。

【解決手段】 平文データ又は暗号文の処理単位データに対応した非反転データ又はその全ビットの反転データのいずれか一方をランダムに取り込み、かかるデータを上記非反転データに対応した転置・換字処理を行うポジ用スクランブル信号処理と、上記反転データに対応した転置・換字処理を行うネガ用スクランブル信号処理とを並列的に行ない、それぞれに対応した出力信号のいずれか一方を上記第1信号処理でのデータ選択動作に対応させて取り出す動作を複数回行なって最後の転置・換字の結果を暗号化データ又は復号化データとする。



1

【特許請求の範囲】

【請求項 1】 平文データ又は暗号文の処理単位データに対応した非反転データ又はその全ビットの反転データのいずれか一方をランダムに取り込む入力選択回路と、上記入力選択回路を通したデータを受け、上記非反転データに対応した転置・換字処理を行うポジ用スクランブル回路と、
上記入力選択回路を通したデータを受け、上記反転データに対応した転置・換字処理を行うネガ用スクランブル回路と、
上記ポジ用スクランブル回路又はネガ用スクランブル回路で転置・換字処理された出力信号のいずれか一方を上記入力選択回路の選択動作に対応させて取り出す出力選択回路と、
上記ポジ用スクランブル回路及びネガ用スクランブル回路での複数回の転置・換字の結果を最終転置する出力回路とを備え、
上記出力回路を通して暗号文又は平文データを得ることを特徴とする暗号化・復号化装置。

【請求項 2】 請求項 1 において、
符号ビットを上記平文データ又は暗号文に対して付加する回路を更に含み、
ランダムに発生される選択信号を上記入力選択回路に供給して、上記符号ビットを含めて非反転データ又はその全ビットの反転データのいずれか一方を取り込むようにし、
上記符号ビットを分離して上記データを上記ポジ用スクランブル回路及びネガ用スクランブル回路で転置・換字処理し、
上記分離された符号ビットを用いて、上記出力選択回路を制御して入力選択回路で取り込まれた非反転データ又はその全ビットの反転データに対応した上記転置・換字処理された出力信号を取り出すことを特徴とする暗号化・復号化装置。

【請求項 3】 請求項 1 又は 2 において、
上記転置・換字処理は、DES 暗号・復号アルゴリズムにより行われるものであることを特徴とする暗号化・復号化装置。

【請求項 4】 請求項 2 又は 3 において、
上記ランダムに発生される選択信号は、乱数発生回路で形成された 1 ビットの 2 値信号を受けて、その論理 1 と論理 0 の出現率がほぼ $1/2$ に補正する補正回路で形成されることを特徴とする暗号化・復号化装置。

【請求項 5】 平文データ又は暗号文の処理単位データに対応した非反転データ又はその全ビットの反転データのいずれか一方をランダムに取り込む第 1 信号処理と、
上記第 1 信号処理で取り込まれたデータを上記非反転データに対応した転置・換字処理を行うポジ用スクランブル信号処理と、上記反転データに対応した転置・換字処理を行うネガ用スクランブル信号処理とを並列的に行な

2

う第 2 信号処理と、

上記ポジ用スクランブル信号処理又はネガ用スクランブル信号処理で転置・換字処理された出力信号のいずれか一方を上記第 1 信号処理でのデータ選択動作に対応させて取り出す第 3 信号処理と、

を複数回行ない、最後の転置・換字の結果を暗号化データ又は復号化データとしてなることを特徴とする暗号化・復号化方法。

【請求項 6】 請求項 5 において、

上記平文データ又は暗号文に対して符号ビットを付加する動作と、

ランダムに発生される選択信号を形成する動作とを更に含み、

上記第 1 信号処理において、選択信号を用いて上記符号ビットを含めて非反転データ又はその全ビットの反転データのいずれか一方を取り込むようにし、

上記第 2 信号処理において、符号ビットを分離して上記ポジ用とネガ用のスクランブル信号処理を行ない、

上記第 3 信号処理において、上記分離された符号ビットを用いて上記第 1 信号処理において取り込まれた非反転データ又はその全ビットの反転データに対応した上記転置・換字処理された出力信号を取り出すようにしてなることを特徴とする暗号化・復号化方法。

【請求項 7】 請求項 5 又は 6 において、

上記転置・換字処理を DES 暗号・復号アルゴリズムにより行うようにしてなることを特徴とする暗号化・復号化方法。

【請求項 8】 請求項 6 又は 7 において、

上記ランダムに発生される選択信号は、乱数発生回路で形成された 1 ビットの 2 値信号の論理 1 と論理 0 の出現率がほぼ $1/2$ に補正するような信号処理が行われることを特徴とする暗号化・復号化方法。

【請求項 9】 入力されたデータに対し、所定の回数だけ所定の変換処理を行うことで、入力されたデータに対応した暗号化されたデータを得るデータの暗号化方法であって、

上記所定の変換処理は、論理 0 又は論理 1 のいずれかの状態をとる制御信号が入力され、入力データの全ビットを反転しない入力データについての処理を行ない第 1 のデータを生成し、入力データの全ビットを反転した入力データについての処理を行ない第 2 のデータを生成し、上記制御信号の状態に応じて、上記第 1 データと上記第 2 データのいずれかを上記所定の変換処理の出力として出力し、

上記第 1 のデータの生成と上記第 2 データの生成とは並列的に行われ、

上記制御信号のとり状態は、論理 0 又は論理 1 のそれぞれの出現比率がおおよそ 50% となるように制御されていることを特徴とするデータの暗号化方法。

【請求項 10】 請求項 9 において、

3

上記制御信号のとり状態が、論理 0 又は論理 1 のそれぞれの出現比率がおおよそ 50% となるように制御するための制御装置を用いることを特徴とするデータの暗号化方法。

【請求項 11】 請求項 10 において、
上記制御装置は、乱数発生装置を有することを特徴とするデータの暗号化方法。

【請求項 12】 外部端子がリードライト装置と電氣的に接続されることによって動作電圧が供給され、かつ、中央処理装置からの指示を受けて動作する暗号処理用演算ユニットによる暗号化処理又は復号化処理を伴ったデータの入出力動作を含む IC カードであって、
上記暗号処理用演算ユニットは、
平文データ又は暗号文の処理単位データに対応した非反転データ又はその全ビットの反転データのいずれか一方をランダムに取り込む入力選択回路と、
上記入力選択回路を通したデータを受け、上記非反転データに対応した転置・換字処理を行うポジ用スクランブル回路と、
上記入力選択回路を通したデータを受け、上記反転データに対応した転置・換字処理を行うネガ用スクランブル回路と、
上記ポジ用スクランブル回路又はネガ用スクランブル回路で転置・換字処理された出力信号のいずれか一方を上記入力選択回路の選択動作に対応させて取り出す出力選択回路と、
上記ポジ用スクランブル回路及びネガ用スクランブル回路での複数回の転置・換字の結果を最終転置する出力回路とを備え、

上記出力回路を通して暗号文又は平文データを得るものであることを特徴とする IC カード。

【請求項 13】 請求項 12 において、
符号ビットを上記平文データ又は暗号文に対して付加する回路を更に含み、
ランダムに発生される選択信号を上記入力選択回路に供給して、上記符号ビットを含めて非反転データ又はその全ビットの反転データのいずれか一方を取り込むようにし、

上記符号ビットを分離して上記データを上記ポジ用スクランブル回路及びネガ用スクランブル回路で転置・換字処理し、

上記分離された符号ビットを用いて、上記出力選択回路を制御して入力選択回路で取り込まれた非反転データ又はその全ビットの反転データに対応した上記転置・換字処理された出力信号を取り出すことを特徴とする IC カード。

【請求項 14】 請求項 12 又は 13 において、
上記転置・換字処理は、DES 暗号・復号アルゴリズムにより行われるものであることを特徴とする IC カード。

4

【請求項 15】 請求項 13 又は 14 において、
上記ランダムに発生される選択信号は、乱数発生回路で形成された 1 ビットの 2 値信号を受けて、その論理 1 と論理 0 の出現率をほぼ 1/2 に補正する補正回路で形成されることを特徴とする IC カード。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】この発明は、暗号化・復号化装置、暗号化・復号化方法、データの暗号化方法及び IC カードに関し、特に IC カードやプログラム内蔵の 1 チップマイクロコンピュータのような CPU とメモリを含み暗号鍵を使ったデータ処理を行なうものの機密保護技術に利用して有効な技術に関するものである。

【0002】

【従来の技術】DES (Data Encryption Standard) は、広範に用いられている秘密鍵ブロック暗号である。DES のアルゴリズムは、大きく平文のデータフローと鍵のデータフローに分割できる。平文データフローでは、IP とよばれる転置 (信号の入れ換え) を行った後、上位と下位それぞれ 32 ビットずつにデータを分割し、転置・換字処理を 16 回繰り返す。最後に上位と下位それぞれ 32 ビットデータを統合し、IP⁻¹ とよばれる転置を行い、暗号文を得る。DES では、暗号化と復号化が同じ処理で実現できる。ただし暗号化と復号化では、鍵のスケジューリングが異なる。鍵のスケジューリング部分について、詳細は省略するが、鍵データを元に、各段に対して 48 ビット鍵スケジューリングデータの出力を行う。

【0003】通常の DES アルゴリズムでは、同じ平文に対しては常に同じ内部動作を行う。その結果、内部信号が入力信号に依存して変化するので、DPA (Differential Power Analysis) 法での統計処理を行いやすい。つまり、DPA 法では、消費電流波形を統計処理して暗号鍵を推定し、例えば DES のある部分に仮定した暗号鍵を当てはめて、平文を変化させながら消費電流波形を測定して統計する。暗号鍵を様々に変化させながらこの作業を繰り返し、正しい鍵のときには電流波形が大きなピークを示す。

【0004】上記のような DPA による DES 解読に対する対策の例として、特開 2000-066585 号公報がある。この公報に記載の技術では、マスク a のパターンと、そのビット反転のマスクパターンのペアを設け、暗号化を行う毎にこのペアの一方をスイッチによりランダムに選択して、装置内部の平文に依存したビットをマスクし、暗号文を出力する前に暗号文からマスク a の影響を除去するようにするものである。

【0005】上記公報に記載の技術では、本来のデータにマスクし、各 S 箱に入力する直前でそのマスクを解除する。このマスクを解除したときに DPA により解読される恐れがあるので、S 箱への入力直前におけるマスク

5

解除、マスク解除後の本来のデータによるS箱への入力、及びS箱からの出力のマスク操作を、事前に計算し、テーブルとして記憶し、テーブル参照することにより計算結果を求めるのでマスク解除のための排他的論理和の計算や、マスクをかけるための排他的論理和の計算が行われることはないのでDPAによる解説を不可能にすることができる説明されている。

【0006】

【発明が解決しようとする課題】しかしながら、上記公報の技術では、排他的論理和の計算を事前にテーブルとして記憶させる構成であり、上記マスクの機能を十分に発揮させるために本来のデータに相当するようなビットにする必要があり、その組み合わせも膨大になるので、かかる膨大な組み合わせからなるマスクに対応した演算結果を格納するテーブル（記憶回路）の回路規模が大きくなってしまふ。また、DPAによる解説防止のためには、上記マスクが特定のパターンに偏らないようにする必要のあることは説明されているが、どのようにすれば複数ビットのパターンが偏らないようにできることの具体的な記述はなく、DPAによる解説の可能性を残している。

【0007】この発明の目的は、簡単な構成で安定的に機密保護の強化を実現した暗号化・復号化装置、暗号化・復号化方法及びICカードを提供することにある。この発明の前記ならびにそのほかの目的と新規な特徴は、本明細書の記述および添付図面から明らかになるであろう。

【0008】

【課題を解決するための手段】本願において開示される発明のうち代表的なものの概要を簡単に説明すれば、下記の通りである。すなわち、入力選択回路において、平文データ又は暗号文の処理単位データに対応した非反転データ又はその全ビットの反転データのいずれか一方をランダムに取り込み、かかる入力選択回路を通したデータを上記非反転データに対応した転置・換字処理を行うポジ用スクランブル回路及び反転データに対応した転置・換字処理を行うネガ用スクランブル回路に伝え、出力選択回路により上記ポジ用スクランブル回路又はネガ用スクランブル回路で転置・換字処理された出力信号のいずれか一方を上記入力選択回路の選択動作に対応させて取り出し、出力回路により上記ポジ用スクランブル回路及びネガ用スクランブル回路での複数回の転置・換字の結果を最終転置して暗号文又は平文データを得る。

【0009】本願において開示される発明のうち他の代表的なものの概要を簡単に説明すれば、下記の通りである。すなわち、平文データ又は暗号文の処理単位データに対応した非反転データ又はその全ビットの反転データのいずれか一方をランダムに取り込み、かかるデータを上記非反転データに対応した転置・換字処理を行うポジ用スクランブル信号処理と、上記反転データに対応した

6

転置・換字処理を行うネガ用スクランブル信号処理とを並列的に行ない、それぞれに対応した出力信号のいずれか一方を上記第1信号処理でのデータ選択動作に対応させて取り出す動作を複数回行ない、最後の転置・換字の結果を暗号化データ又は復号化データとする。

【0010】

【発明の実施の形態】図1には、この発明に係る暗号化・復号化装置、暗号化・復号化方法及びICカードに適合されたDES暗号コプロセッサの一実施例の概略ブロック図が示されている。この実施例では、DES暗号コプロセッサ内の平文信号（データ）1に1ビットからなる符号ビット2を付加して内部演算用信号3とする。上記符号ビットが“0”のとき、平文信号はポジ（信号値が平文値そのもの）を表す。符号ビットが“1”のときはネガ（信号値の反転値が平文値）を表す。平文信号および符号ビットは、演算ごとに反転用乱数信号4によって、排他的論理和5で内部演算信号全ビットを反転させる。

【0011】スクランブル回路はポジ信号用6とネガ信号用7の2種類が別々に用意されており、符号ビット2の値により、ポジ信号用6とネガ信号用7の各出力信号をセレクタ8を用いて選択する。このような回路での16回の繰り返し演算のあと、暗号データの出力の前に排他的論理和9を置き、符号ビット2が“1”なら暗号データを反転させる。

【0012】図2には、本暗号コプロセッサが処理する暗号方式である、DES暗号のアルゴリズムを説明するための構成図が示されている。DESの暗号化／復号化演算は、64ビットの平文（暗号化の対象となるデータ）あるいは64ビットの暗号文と、56ビットの鍵を用いて行われる。

【0013】DESのアルゴリズムは、大きく平文のデータフローと鍵のデータフローに分割できる。平文データフローでは、IPとよばれる初期転置（信号の入れ換え）を行った後、上位と下位それぞれ32ビットずつにデータを分割し、図3で示された転置・換字処理を16回繰り返す。最後に上位と下位それぞれ32ビットデータを統合し、IP⁻¹とよばれる転置を行い、暗号文を得る。

【0014】DESでは、暗号化と復号化が同じ処理で実現できる。ただし暗号化と復号化では、鍵のスケジューリングが異なる。鍵のスケジューリング部分について、詳細は省略するが、鍵データを元に、各段に対して48ビット鍵スケジューリングデータの出力を行う。

【0015】図3に示された16回の繰り返し演算部分は、転置処理、排他的論理和演算、およびSBOXとよばれる換字処理で構成されている。SBOXは入力48ビット、出力32ビットの、変換テーブルを元にした換字処理である。SBOXの変換テーブルは、FIPS-46やANSI-80、ISOでその内容が定義されて

7

いる。SBOXの内部は、図4に示されているように、S1からS8の8つの換字処理部に分割される。それぞれの換字処理は、入力6ビット、出力4ビットである。

【0016】上記のようなDESアルゴリズムをそのままハードウェア化した際に問題点となるのは、DPA (Differential Power Analysis) による電流解析に弱い点である。DPAアタックは、チップの消費電流波形から暗号鍵の値を推定する解析手法である。DPAでは、アタッカーはまずチップに平文データを与え、そのデータを処理する際の消費電流波形を計測する。次に、チップ内部に納められた秘密鍵の値 (の一部) を仮定し、着目した信号線の変化 (=消費電流の微小増加) の予測を、実際の消費電流波形に適用する。仮定した鍵が正しい場合、消費電流の増加が増幅され、ピークとなって表れる。DES暗号は元々、ハードウェア化が容易になるよう設計されたアルゴリズムである。そのためDES暗号処理用のハードウェアを設計すると、どの製品でも似たような内部構造となる。これがDPAによる解析を容易にしている。

【0017】DPAによる解析を困難にする方法として、前記のように特開2000-066585号公報のように、演算ごとに内部データや処理内容を変化させるという方法がある。内部データを毎回変える方法で簡単なのは、平文に何らかのスクランブル用コードとの排他的論理和をかける方法である。しかしこの方法だと、転置処理を行う度に、データにかかっているスクランブルコードの値が変わる。そのため、演算データにかかっているスクランブルコードの値を保持しておく必要がある。

【0018】この発明では、演算データの全ビットを反転させるか否かをランダムに決定する方式をとる。この方式だと、演算データに1ビットの符号データを付与するだけで、現在の演算データの状態 (反転/非反転) を保持できる。また、転置と排他的論理和の影響を受けない。ただし、SBOXだけは反転データと非反転データで変換テーブルが異なるため、非反転データ用 (通常のSBOX) と、本願によって追加された反転データ用 (SBOX-BAR) の二種類のSBOXが用意される。そして符号ビットにより、SBOXとSBOX-BARのどちらを使用するかを選択する。つまり、2つのSBOXとSBOX-BARのいずれか一方の出力信号を有効として取り出す。

【0019】上記SBOXの作り方を、S1を例に説明すると次の通りである。DES規格に基づくS1の換字構成を図5に示す。図5 (a) の横方向が入力6ビット中4ビットで表される数字 (0~15)、縦方向が入力の残り2ビット (0~3)、書かれている数字がその入力に対する出力4ビット (0~15) を表している。反転データ用S1-BARは、図6 (b) に示すように、論理的にはS1の入力と出力両方を反転させることで作

8

成する。図5 (b) にS1-BARの換字構成が示されている。図5 (a) 左上の"14"は、入力が"000000"のときの出力値を表している。この出力に対応するS1-BARは、図5 (b) の右下 (入力"111111"に相当) の、"14"を反転させた"1"にあたる。

【0020】実際のコプロセッサに組み込むのは、図5 (b) のように再計算した換字構成である。すなわち、図6 (a) の非反転データ用に対応したSBOXに対して、図6 (b) に示したように、同じSBOXに対して入力と出力にインバータ回路を設けたような論理をそのまま使用するわけではない。

【0021】本発明の変形例としては、図7 (a) 示したように入力側のみにインバータ回路を設けたSBOX、あるいは図7 (b) に示したように出力側のみにインバータ回路を設けたSBOXと等価な換字構成 (表) を用いたSBOXのペアを使用することも可能である。

【0022】図8には、本発明に係る暗号化・復号化装置、暗号化・復号化方法を説明するための基本構造 (平文の転置・換字処理部分) の一実施例のブロック図が示されている。IP、IP⁻¹、鍵スケジューリング部は、前記図2ないし図4を用いて説明したDESの基本アルゴリズムと同じなので、その説明を省略する。図8において、Aで表される個所が図1において演算データを反転か否かをランダムに決定する部分、Bで表される個所が2つのSBOXの出力を選択する部分である。

【0023】図8において、Aの部分にインバータ回路を通した反転信号と、その入力信号とを選択信号で制御されるマルチプレクサで出力させるように示されているが、図9で示したように、1ビットの選択信号を共通に受ける排他的論理和を使用しても等価な回路が構成できる。つまり、符号ビットを含んだ33ビットの入力データは、選択信号が論理0ならそのまま出力され、選択信号が論理1なら上記33ビットの入力信号が反転されて出力される。図8のようにインバータ回路とマルチプレクサを用いた場合でも、図9のように排他的論理和回路を用いた場合でも、MOSFETで構成した場合には基本的にはほぼ同じ回路素子で構成できるのでいずれを選んでも大差はない。

【0024】図10には、演算データ反転部分のデータフローを説明するためのブロック図が示されている。図10 (a) は、選択信号、つまりデータの反転/非反転を決定する乱数信号の値が"0"のときの動作を示している。図10 (b) は、選択信号が"1"のときの動作を示している。前段から来るデータをMとすると、選択信号が"0"のときには、図10 (a) のように、拡大転置Eに入るデータはMが選択される。選択信号が"1"のときには、図10 (b) のように、拡大転置Eに入るデータとしてMB (Bは図10 (b) の反転信号であるバーを表している) が選択される。拡大転置Eの出

力はそれぞれE (M)、E (MB)となる。拡大転置Eは信号の並び換え処理なので、E (MB)はE (M) Bと等しい。結局、Mに対する拡大転置Eの出力は、選択信号=" 0" のときにE (M)、選択信号=" 1" のときにE (M) の反転値となる。

【0025】図11には、SBOX出力選択部分のデータフローを説明するためのブロック図が示されている。出力の選択は、SBOXに入るデータの符号ビットによって行われる。図11 (a) に示すように、SBOXに10 入力されるデータがX (符号信号=" 0") の場合、非反転データ用のSBOXの出力が選択される。図11

(b) に示すように、入力信号がXB (Xの反転データ、符号信号=" 1") の場合、反転データ用のSBOX-BARの出力が選択される。

【0026】図12には、データの反転/非反転用の選択信号を形成する回路の一実施例のブロック図が示されている。この実施例では、選択信号として、ICカードに搭載されている乱数発生器の非同期発振信号を使用している。ただし非同期発振信号は温度や電圧によって出力に偏りがでるため、補正回路を介してから使用している。20 補正回路により、非同期発振信号が0あるいは1にスタックした場合でも、0/1の比率が50%に近い信号を選択信号として使用することができる。

【0027】図13には、この発明に用いられる0/1比率補正回路の一実施例のブロック図が示されている。この実施例では、8段のシフトレジスタがリング状に接続される。シフトレジスタの初段回路B1には、その出力信号と最終段B8の出力信号との排他的論理和が採られて入力信号とされる。第2段目B2の出力信号は、乱数発生器より供給される非同期発振信号の出力と排他的20 論理和が採られて第3段目B3の入力信号とされる。以下、第3段目B3から最終段B8までは順次に伝えられる。そして、特に制限されないが、第6段目B6の出力信号が選択信号として用いられる。

【0028】この実施例では、シフトレジスタB2~B8で記憶されたビットが連続して同じ値になったときに、B1での排他的論理和処理により適宜反転させ、かつ乱数発生器からの非同期発振信号が連続して、論理0又は1に偏った場合にも、シフト段B2とB3の間で適宜に反転させて、論理0と論理1の出現率を50%ずつ40 に補正するものである。

【0029】本発明において、耐DPA強度を決定するのが、反転/非反転用の選択信号である。チップ内部信号の0/1出現比率を50%に近くすることで、DPAによる解析を困難にすることが可能となる。つまり、前記のようにDPAでは、データを処理する際の消費電流波形を計測して統計的手法によってピークを探すので、上記0/1出現比率を50%にすることにより、統計処理での消費電流が平均化されてピークが無くなってしま40 うので、かかるDPAによる解釈が困難になるものであ

る。

【0030】この実施例では、前記説明したように、平文データに符号ビットを付加し、ポジ/ネガの両方の状態を持つようにする。暗号化における繰り返し演算時に、データを符号ごとランダムに変更する。符号の影響を受けない演算(排他的論理和など)はそのまま符号を無視して演算する。符号の影響を受ける演算(変換表を用いた演算など)では、ポジ用の演算回路とネガ用の演算回路を用意し、データの符号によって演算回路の出力を選択する機構を用いる。

【0031】この実施例に従えば、暗号演算時間が増加しない。例えばダミーの演算を行うなど、演算時間を延ばして攪乱する方法もあるが、本方法は演算するたびに内部処理内容が異なるという攪乱方法をとっているため、1回の演算にかかる時間は未対策のときと同じである。そして、この実施例では、DPA対策をハードウェアに盛り込んでいるので、ソフトウェアにより対策を採る場合のようにユーザに余分な負荷をかけない。

【0032】図14には、この発明が適用されるICカードの一実施例の外観図が示されている。ICカードは、プラスチックケースからなるカード101と、かかるカード101の内部に搭載された図示しない1チップのマイクロコンピュータ等からなるICカード用チップを持つものである。上記ICカードは、さらに上記ICカード用チップの外部端子に接続されている複数の接点(電極)102を持つ。複数の接点102は、後で図15によって説明するような電源端子VCC、電源基準電位端子VSS、リセット入力端子RESバー、クロック端子CLK、データ端子I/O-1/IRQバー、I/O-2/IRQバーとされる。ICカードは、かかる接点102を通して図示しないリーダーライタのような外部結合装置から電源供給を受け、また外部結合装置との間でのデータの通信を行う。

【0033】図15には、この発明に係るICカードに搭載されるICカード用チップ(マイクロコンピュータ)の一実施例の概略ブロック図が示されている。同図の各回路ブロックは、公知のMOS集積回路の製造技術により、特に制限されないが、単結晶シリコンのような1個の半導体基板上において形成される。

【0034】この発明に係るICカード用チップの構成は、基本的にマイクロコンピュータと同じような構成である。その構成は、クロック生成回路、中央処理装置(以下、単にCPUという)、ROM(Read Only Memory)やRAM(Random Access Memory)、不揮発性メモリ(EEPROM)などの記憶装置、暗号化及び復号化処理の演算を行なうコプロセッサ(暗号化・復号化装置)、入出力ポート(I/Oポート)などからなる。

【0035】クロック生成回路は、図示しないリーダーライタ(外部結合装置)から図1の接点102を介して供給される外部クロックCLKを受け、かかる外部クロッ

11

ク信号に同期したシステムクロック信号を形成し、それをチップ内部に供給する回路である。CPU201は、論理演算や算術演算などを行う装置であり、システムコントロールロジック、乱数発生器及びセキュリロジック及びタイマなどを制御する。RAM、ROM、EEPROMのような記憶装置は、プログラムやデータを格納する装置である。コプロセッサは、前記説明したよう

10 DES暗号法などに適合された回路から構成される。I/O（入出力）ポートは、リーダライタと通信を行う装置である。データバスとアドレスバスは、各装置を相互に接続するバスである。

【0036】上記記憶装置のうち、ROMは、記憶内容が不揮発的に固定されているメモリであり、主にプログラムを格納するメモリである。揮発性メモリ（以下、RAMという）は自由に記憶情報の書き換えができるメモリであるが、電源の供給が中断されると、記憶している内容が消えてなくなる。ICカードがリーダライタから抜かれると電源の供給が中断されるため、上記RAMの内容は、保持されなくなる。

【0037】上記不揮発性メモリ（以下、EEPROM (Electrical Erasable Programmable Read Only Memory) という）は、内容の書き換えが可能な不揮発性メモリであり、その中に一旦書き込まれた情報は、電源の供給が停止されてもその内部に保持される。このEEPROMは、書き換える必要があり、かつICカードがリーダライタから抜かれても保持すべきデータを格納するために使われる。例えば、ICカードがプリペイドカードとして使用されるような場合、のプリペイドの度数などは、使用するたびに書き換えられる。この場合の度数などは、リーダライタが抜かれてもICカード内で記憶保持する必要があるため、EEPROMで保持される。

30

【0038】CPUは、いわゆるマイクロプロセッサと同様な構成にされる。すなわち、その詳細を図示しないけれども、その内部に命令レジスタ、命令レジスタに書込まれた命令をデコードし、各種のマイクロ命令ないしは制御信号を形成するマイクロ命令ROM、演算回路、汎用レジスタ（RG6等）、内部バスBUSに結合するバスドライバ、バスレシーバなどの入出力回路を持つ。CPUは、ROMなどに格納されている命令を読み出し、その命令に対応する動作を行う。CPUは、I/O

40

ポートを介して入力される外部データの取り込み、ROMからの命令や命令実行のために必要となる固定データのようなデータの読み出し、RAMやEEPROMに対するデータの書き込みと読み出し動作制御等を行う。

【0039】上記CPUは、クロック生成回路から発生されるシステムクロック信号を受けそのシステムクロック信号によって決められる動作タイミング、周期をもって動作される。CPUは、その内部の主要部がPチャンネル型MOSFETとNチャンネル型MOSFETとからなるCMOS回路から構成される。特に制限されない

50

12

が、CPUは、CMOSスタティックフリップフロップのようなスタティック動作可能なCMOSスタテック回路と、信号出力ノードへの電荷のプリチャージと信号出力ノードへの信号出力とをシステムクロック信号に同期して行うようなCMOSダイナミック回路とを含む。

【0040】コプロセッサは、前記説明したように内部で扱う平文データに符号ビットを付加し、ポジ／ネガの両方の状態を持つようにする。暗号化における繰り返し演算時に、データを符号ごとランダムに変更する。符号の影響を受けない演算（排他的論理和など）はそのまま符号を無視して演算する。符号の影響を受ける演算（変換表を用いた演算など）では、ポジ用の演算回路とネガ用の演算回路を用意し、データの符号によって演算回路の出力を選択する機構を用いる。

【0041】この実施例のICカードにおいても、演算するたびに内部処理内容が異なるという攪乱方法をとっているため、1回の演算にかかる時間は未対策のときと同じであるので、高速なデータ処理が可能であり、DPA対策をハードウェアに盛り込んでいるので、DPA対策のためにCPUが余分な動作を行う必要がないのでユーザに余分な負荷をかけなくて済む。

【0042】上記の実施例から得られる作用効果は、下記の通りである。すなわち、

(1) 入力選択回路において、平文データ又は暗号文の処理単位データに対応した非反転データ又はその全ビットの反転データのいずれか一方をランダムに取り込み、かかる入力選択回路を通したデータを上記非反転データに対応した転置・換字処理を行うポジ用スクランブル回路及び反転データに対応した転置・換字処理を行うネガ用スクランブル回路に伝え、出力選択回路により上記ポジ用スクランブル回路又はネガ用スクランブル回路で転置・換字処理された出力信号のいずれか一方を上記入力選択回路の選択動作に対応させて取り出し、出力回路により上記ポジ用スクランブル回路及びネガ用スクランブル回路での複数回の転置・換字の結果を最終転置して暗号文又は平文データを得ることにより、簡単な構成で高速にしかも安定的にDPA対策による機密保護を実現できるという効果が得られる。

【0043】(2) 上記に加えて、符号ビットを上記平文データ又は暗号文に対して付加し、ランダムに発生される選択信号を上記入力選択回路に供給して、上記符号ビットを含めて非反転データ又はその全ビットの反転データのいずれか一方を取り込むようにし、上記符号ビットを分離して上記データを上記ポジ用スクランブル回路及びネガ用スクランブル回路で転置・換字処理し、分離された上記符号ビットを用いて、上記出力選択回路を制御して入力選択回路で取り込まれた非反転データ又はその全ビットの反転データに対応した上記転置・換字処理された出力信号を取り出すことにより、簡単な構成によりDPA対策を実現できるという効果が得られる。

【0044】(3) 上記に加えて、上記転置・換字処理をDES暗号・復号アルゴリズムにより行うようにすることにより、暗号化と復号化が同じ処理で実現できるから回路の簡素化が可能になるという効果が得られる。

【0045】(4) 上記に加えて、ランダムに発生される選択信号を、乱数発生回路で形成された1ビットの2値信号を受けて、その論理1と論理0の出現率をほぼ1/2に補正するという簡単な回路を付加することにより、より強固なDPA対策を実現できるという効果が得られる。

【0046】以上本発明者よりなされた発明を実施例に基づき具体的に説明したが、本願発明は前記実施例に限定されるものではなく、その要旨を逸脱しない範囲で種々変更可能であることはいうまでもない。例えば、ICカードには、1つの半導体集積回路装置を搭載するもの他、複数の半導体集積回路装置が搭載されるものであってもよい。暗号化・復号化装置が搭載されるマイクロコンピュータは、1つの半導体集積回路装置に形成されるもの他、CPUとその周辺回路が複数チップで構成されて、1つのモジュール基板に搭載されてなるものであってもよい。

【0047】上記マイクロコンピュータは、データ処理装置とかかるデータ処理装置によるデータ処理手順が書き込まれたROMを含んで上記データ処理手順に従ってデータの入出力動作が行われるものであれば何であってよい。例えば、前記のようなICカード用チップの他に、ゲーム用等の1チップマイクロコンピュータ等のように機密保護の必要な各種マイクロコンピュータに広く適用できるものである。この発明は、暗号化・復号化装置、暗号化・復号化方法、データの暗号化方法及び機密保護を必要とする各種ICカードやマイクロコンピュータに広く利用できる。

【0048】

【発明の効果】本願において開示される発明のうち代表的なものによって得られる効果を簡単に説明すれば、下記の通りである。すなわち、入力選択回路において、平文データ又は暗号文の処理単位データに対応した非反転データ又はその全ビットの反転データのいずれか一方をランダムに取り込み、かかる入力選択回路を通したデータを上記非反転データに対応した転置・換字処理を行うポジ用スクランブル回路及び反転データに対応した転置・換字処理を行うネガ用スクランブル回路に伝え、出力選択回路により上記ポジ用スクランブル回路又はネガ用スクランブル回路で転置・換字処理された出力信号のいずれか一方を上記入力選択回路の選択動作に対応させて取り出し、出力回路により上記ポジ用スクランブル回路及びネガ用スクランブル回路での複数回の転置・換字の結果を最終転置して暗号文又は平文データを得ることにより、簡単な構成で高速にしかも安定的にDPA対策による機密保護を実現できる。

【図面の簡単な説明】

【図1】この発明に係る暗号化・復号化装置、暗号化・復号化方法及びICカードに適合されたDES暗号コプロセッサの一実施例を示す概略ブロック図である。

【図2】この発明に用いられるDES暗号のアルゴリズムを説明するための構成図である。

【図3】この発明に用いられるDES暗号のアルゴリズムにおける演算部分を説明するためのブロック図である。

10 【図4】この発明に用いられるDES暗号のアルゴリズムにおけるSBOXの内部を説明するための構成図である。

【図5】この発明に用いられるDES暗号のアルゴリズムにおけるSBOXの作り方を、S1を例にした説明図である。

【図6】この発明に係るSBOXの作り方を、S1を例にして論理的に説明するための説明図である。

20 【図7】この発明に係るSBOXの作り方の他の一例を、S1を例にして論理的に説明するための説明図である。

【図8】本発明に係る暗号化・復号化装置、暗号化・復号化方法を説明するための基本構造（平文の転置・換字処理部分）の一実施例を示すブロック図である。

【図9】本発明に係る暗号化・復号化装置、暗号化・復号化方法における入力選択回路の他の一実施例を説明するためのブロック図である。

【図10】本発明に係る暗号化・復号化装置、暗号化・復号化方法における演算データ反転部分のデータフローを説明するためのブロック図である。

30 【図11】本発明に係る暗号化・復号化装置、暗号化・復号化方法におけるSBOX出力選択部分のデータフローを説明するためのブロック図である。

【図12】本発明に係る暗号化・復号化装置、暗号化・復号化方法におけるデータの反転／非反転用の選択信号を形成する回路の一実施例を示すブロック図である。

【図13】この発明に用いられる0/1比率補正回路の一実施例を示すブロック図である。

【図14】本発明に係るICカードの一実施例を示す外觀図である。

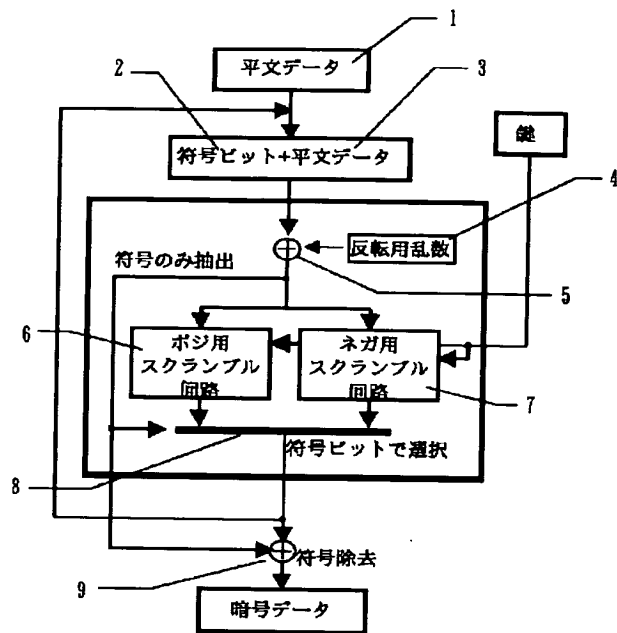
40 【図15】本発明に係るICカードに搭載されるICカード用チップ（マイクロコンピュータ）の一実施例を示す概略ブロック図である。

【符号の説明】

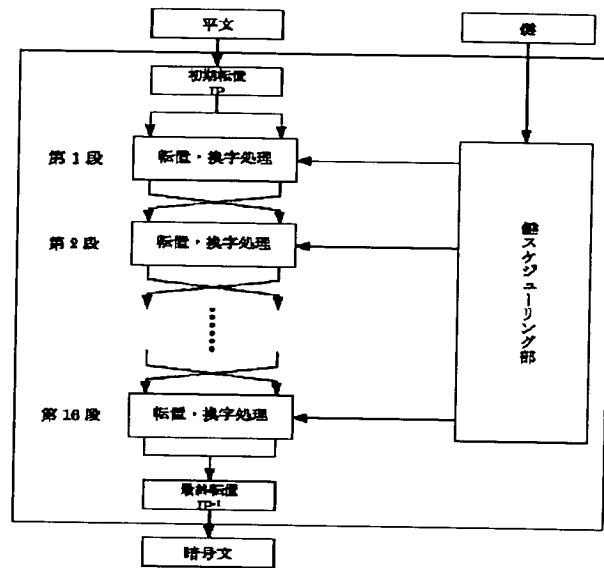
1…平分信号、2…符号ビット、3…内部演算用信号、4…反転用乱数信号、5…排他的論理和、6…ポジ用スクランブル回路、7…ネガ用スクランブル回路、8…セレクト、9…排他的論理和、101…カード、102…接点

RAM・ランダム・アクセス・メモリ、ROM…リード・オンリ・メモリ、EEPROM…不揮発性メモリ、

【図1】

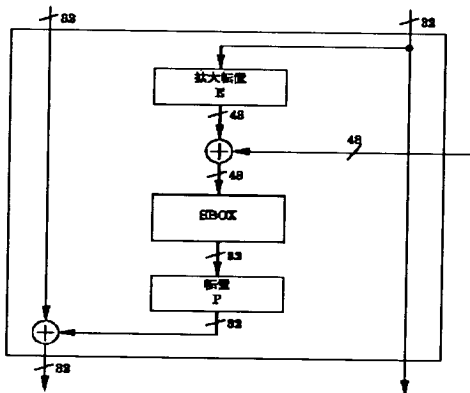


【図2】

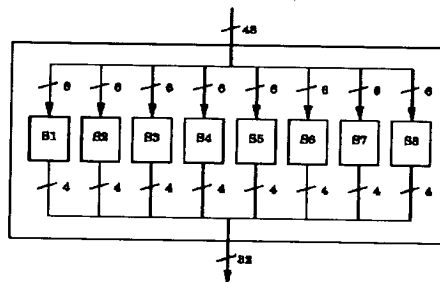


【図9】

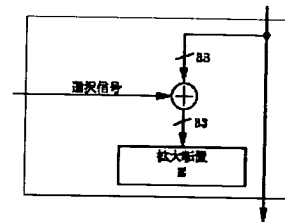
【図3】



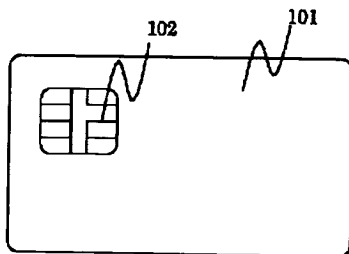
【図4】



【図5】



【図14】



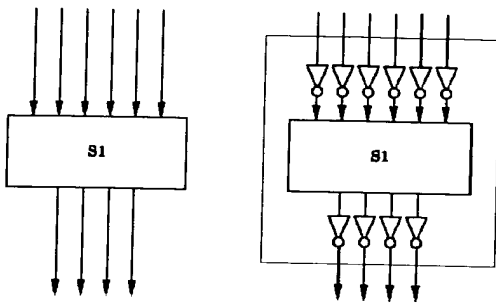
(a) Sボックス(S1)の換字表

14	4	18	1	2	16	11	8	8	10	6	12	5	9	0	7
0	15	7	4	14	2	18	1	10	6	12	11	9	5	3	8
4	1	14	8	13	6	2	11	16	13	9	7	3	10	5	5
15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	18

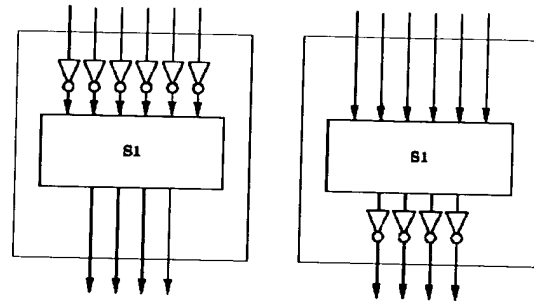
(b) SボックスBAR(S1-BAR)の換字表

2	9	15	6	1	12	4	10	8	14	6	11	13	7	3	0
15	10	5	12	8	6	8	0	4	18	9	2	7	1	14	11
7	12	10	6	4	8	9	5	14	2	13	1	11	8	0	15
8	18	6	10	8	9	5	12	7	4	0	18	14	2	11	1

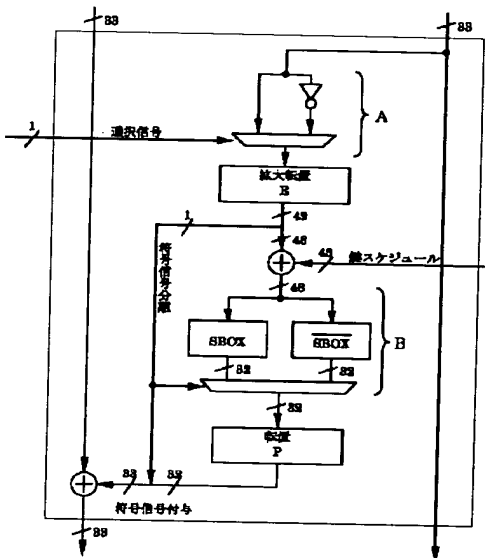
【図6】



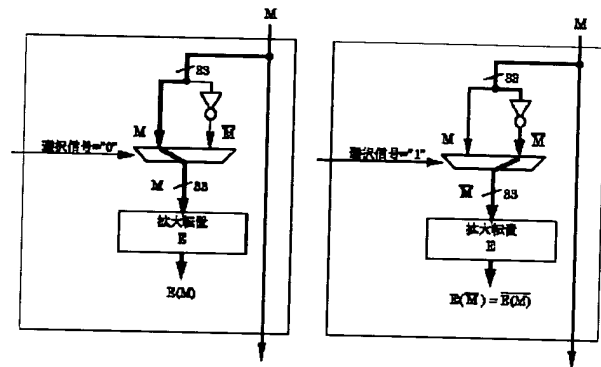
【図7】



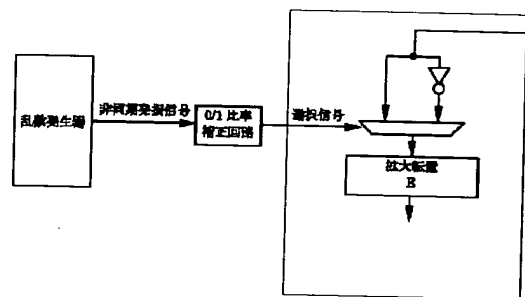
【図8】



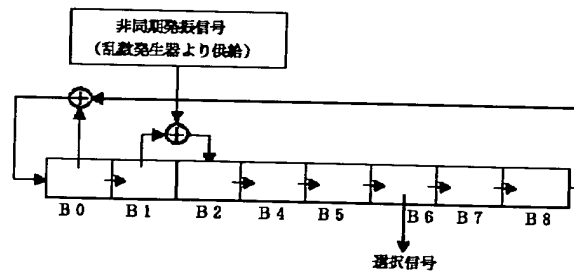
【図10】



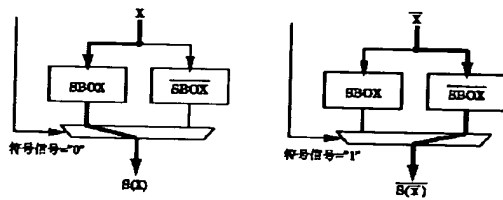
【図12】



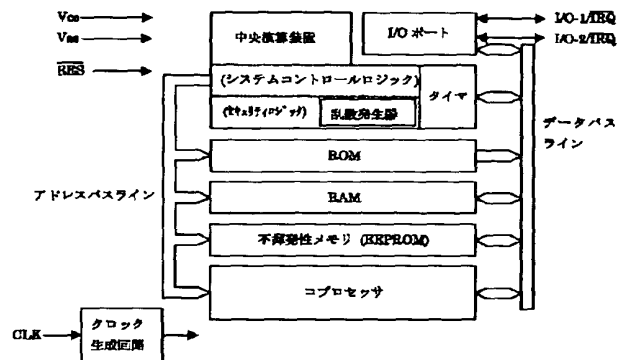
【図13】



【図11】



【図15】



フロントページの続き

(72) 発明者 ▲高▼橋 雅聡
 東京都小平市上水本町5丁目22番1号 株
 式会社日立超エル・エス・アイ・システム
 ズ内

Fターム(参考) 5B035 AA13 BB09 BC02 CA38
 5J064 AA04 BC01 BC02 BC03 BD02
 BD03
 5J104 AA47 JA03 JA13 NA02